WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Video Watermarking Algorithm to Enhance Data Security

[1]Nishad P. Kulkarni, [2]Aditya A. Patil and [3]Dr. M. A. Gangarde

[1,2,3]Pune Institute of Computer Technology, Pune 411043, India

ABSTRACT—

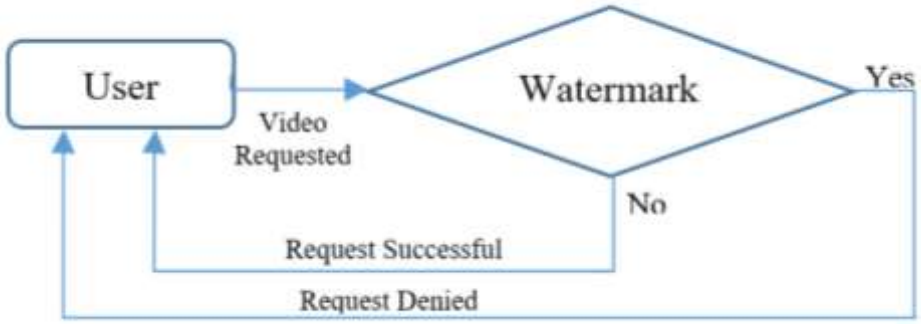
Video Watermarking techniques are mainly developed with the intention to enhance security of videos distributed across media networks. Enhance security refers to as prevention of unauthorized access to the multimedia content. Due to massive transfer of multimedia content across the internet, digital right protection and copyright protection are the most important points that need to be focused on. Various Video Watermarking algorithms which are developed till now lack in various aspects.

When you develop an algorithm, various factors and performance parameters are needed to be considered. Evaluation of performance parameters like NCC, PSNR, BER, WER, SSIM, VIFP, VMAF and many other has to be done.

Keywords—Digital Watermarking, robustness to attacks, copyright protection, payload, blind detection.

I. Introduction

The necessity of secure communication and digital data transmit has potentially increased with the growth of multimedia systems. The main technique used for protection of Intellectual Property and copyright security is digital watermarking. Digital watermarking can be applied to media like text, audio, image, video etc. A watermark is a digital data embedded in multimedia objects and can be extracted later in order to make an assertion about the article. The main reason of digital watermarking is to embed information robustly in the host data. Typically the watermark contains information about the basis, ownership, destination, copy control, transaction etc. The applications of digital watermarking include copy control, authentication, database linking etc. A user's request for a video downloaded can be cancelled if a watermark is detected, or the request can be responded to it if no watermark is detected.



A huge number of watermarking schemes have been proposed to hide copyright marks and other information in digital images, video, audio and other multimedia objects. The pixel value is altered, but the invisible watermark is implanted such that it is undetectable, and it can be recovered only with an appropriate decoding mechanism. If the watermark cannot be easily removed from the watermarked signal even after applying frequent watermarking attacks then it is referred as robust embedding. The watermark must also be capable of identifying the source and intended recipient with a low probability of error.

In this paper, we have compared various techniques, methods and parameters and also figured out the pros and cons with these techniques. While comparing the approaches that were used, we figured out the areas which need to be improved.

II. Related work

L. Rajab, T. Al-Khatib, and A. Al-Haj have worked on lossless efficient video-watermarking technique based on an optimal keyframes selection using IGSA and HT in the LWT domain. In this scheme, a scrambled watermark logo is incorporated into the keyframes followed by a one-level LWT [1]. S. A. Thajeel have worked on Slantlet Transform , sub-bands (i.e., LL, LH, HL, and HH) , Contourlet Transform (CT) , DCT (Discrete Cosine Transform) and , to improve the security and robustness, the watermark logo is scrambled using AT(Arnold transformation) [3].

M. Asikuzzaman and M. R. Pickering have worked on three types of content: MP4, AVI and MPEG footage, and two watermarks are used with each video, enabling us to assess the quality of the watermark in all three formats [11]. P. Khare and V. K. Srivastava have discussed and implemented hybrid watermarking technique based on DWT and SVD has been presented to achieve simultaneously the trade-off between robustness and invisibility. At the sender side, the one-level DWT is used to decompose the original image to seek for the embedding position and then the watermark is inserted. Some key parameters are transmitted through a private channel to later recover the watermark image [10]. M. A. Gangarde and J. S. Chitode have proposed novel and innovative Video Watermarking using Pixel Location Based Technique (PLBT) to improve the robustness and imperceptibility of secret data. They have located the pixel values of selected frames of watermarked video with the obtained pixel values of secret watermark image and locate the respective offset values of selected frames of watermarked video as a secret key [15].

III. Watermarking keywords

1) **Copyright Protection:** A copyright owner can embed watermark containing the copyright information in host video which win decoded can be used as a proof of ownership.

2) **Robustness:** Robustness means the resistance of a watermark to blind non targeted modifications or the common media operations of regular users. These operations are likely to degrade the quality of the video.

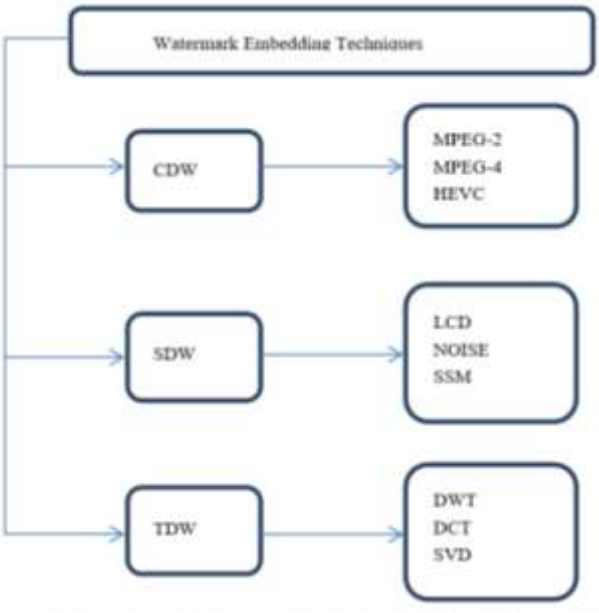
3) **Payload:** Data payload refers to the number of watermarking bits embedded in an image and video. Increasing the payload causes greater visibility of the watermark and vice versa. A watermarking system that embeds multiple bits is refered to as multi-bit watermarking and a zero-bit watermarking system provides access control by checking for the presence of the watermark (Present or Absent)

4) Watermark Embedding Techniques :

a) Compressed Domain Watermarking: The watermark method for this category integrates the watermark into the cover video's compressed domain. Many watermarking algorithms based on MPEG technology are proposed. For copyright protection, a video watermarking system based on MPEG-2 compression is suggested.

b) Spatial Domain Watermarking: The pixels that make up a picture are defined by its spatial domain. By altering the brightness and colour value of a few selected pixels, spatial domain watermarking embeds the watermark. Watermarking in the spatial domain is simpler and its calculating speed is high than transform domain but it is less powerful against attacks.

c) Transform Domain Watermarking: transform domain functions including discrete wavelet transform (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD) with an image as the host signal



5) **Blind Detection:** Digital watermarking is also classified as blind or nonblind.

a) Blind watermarking method: The original video as well as the original watermark are not required at the time of extraction. None of the information of the host is used in extracting the embedded watermark.

b) Nonblind watermarking method: Nonblind watermarking requires the original image to detect to watermark

6) **Video Authentication:** Today's popular video editing programmes enable users to successfully manipulate video material. Therefore, verification techniques are necessary to ensure the content's legitimacy. One solution is the use of sophisticated watermarks. Every frame of the video feed includes a timestamp, camera ID, and casing chronic number as a watermark.

7) Common Attacks:

a) Simple_attacks:

b) Detection_disabling attacks:

c) Ambiguity_attacks:

d) Removal_attacks:

e) Cropping Attack:

f) Copy – Paste Attack:

g) Adding Noise Attack:

8) **Attacks Analysis:** In addition to noise adding attacks, spin attacks, frame assaults, engineering attacks, and JPEG compression attacks as in Source, the most frequent attacks were also addressed. Some attacks still haven't been dealt with. Table 3 lists the assaults on the watermark video in accordance with the sources that were examined and the outcomes. Because low frequencies carry crucial information and may be robust and impervious to assaults, they are preferred because they conceal a method to prevent these attacks..

9) Prevention Methods:

Utilizing pressure reduction techniques from the present era results in storing of secret data in secure locations.

Relying on video frames to conceal with digital audio, in order to conceal secret data as much as feasible..

Due to the video's large file size, data can be stored multiple times even if some of it is lost. By matching the frames, the lost data can be fully recovered.

10) Required Formulas:

a) BER = N_{err} / N_{bits}

b) PSNR = $10\log_{10}((L - 1)^2 / MSE)$

1. L is the number of maximum possible intensity levels (minimum intensity level supposed to be 0) in an image.
2. MSE is the mean squared error

c) WDR = $E_0 * E_1 / M_0 * M_1$

1. E_0 number of extracted zeros
2. E_1 number of extracted ones
3. M_0 number of zeros in watermark
4. M_1 number of ones in watermark

d) SSIM – Structural Similarity Index Metric

$$SSIM(x,y) = \frac{(\mu_x\mu_y + C_1)(\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

e) NC – Normalised Correlation

$$NC = \frac{\sum_1^N \sum_1^M w(i,j)w'(i,j)}{\sqrt{\sum_1^N w(i,j)^2}\ \sqrt{\sum_1^M w'(i,j)^2}}$$

IV. Application

a) Cyber-Security –

Blockchain is a relatively new and promising technology that has the potential to introduce transparency and trust to openly protect a network and validate transactions.

Blockchain and watermarking are directed on the solution of different problems of cyber-security. Their joint use will potentially allow achieving a higher security level than when using the given technologies separately. This idea has already found the reflection in the previous studies; however, mainly only in one direction connected to the problem of digital rights management. Therefore, joint use of the given technologies in other applications is a perspective direction of the research, the development of which would allow bringing the contribution to the important area of cyber-security.

We used blockchain technology to avoid involving a trusted third party for authentication. Secure Hash Algorithm 256 (SHA-256) is applied on the watermark to save it into the blockchain. The watermark is encrypted using Advanced Encryption Standard (AES) and embedded into the image.

b) Fingure Printing –

The focus is to increase the security of the fingerprint image in authentication system. The extraction process doesn't require an original fingerprint. The original fingerprint image is then recovered from the watermarked fingerprint image based on the reversible watermarking technique. The similarity between the reversible fingerprint image and the original is considered, and we could extract minutiae points from it without a problem.

c) Broadcast Monitering –

Broadcast monitoring can be defined the process of tracking and observing activities on broadcasting channels in compliance with intellectual property rights and other illegal activities not conforming to broadcasting laws using the computer or human system. It is also the process of receiving and reviewing media that is transmitted on a broadcast channel to determine if a particular media item has or has not been broadcasted. Broadcast monitoring may be performed to ensure an advertisement has been inserted on a broadcast television system as defined in an advertising agreement or broadcast monitoring may be used to ensure some media is not broadcast (e.g. licensed content).

V. Limitations

Expectation for watermarking techniques should be realistic since watermarking systems deal with a trade-off between robustness, watermark data rate (payload), and imperceptibility. A robust watermark which resists all attacks is not realistic.

Attacks on watermarks may not necessarily remove the watermark, but disable its readability Some Attacks do not remove the watermark, but modify the content so that the detector can no longer find or extract the watermark anymore

To get the most out of video database, it is necessary to improve the image handling processing and the unlimited nature of attacks and the trade-off between visibility and robustness are major challenges of watermarking.

VI. Comparison

Various Video Watermarking Embedding Technique comparison :-

Here is a summary of the comparison of proposed video watermarking technologies in [16] to existing technologies based on the features of the digital watermark in presence of Gaussian noise.

Discrete waveform (DWT) and Single Value Analysis(SVD) improve the exhibition of the watermark embedding process. This demonstrates that the proposed scheme has higher durability and unconsciousness against various image and video processing attacks.

Table 1 shows the Comparison of proposed method with different existing methods [16]

Video	**Σ=0.1**	**Σ=0.5**	**Σ=1**
PSNR (db)	54	53.25	50
NCC	0.97	0.967	0.93
BER	0.01	0.023	0.032

Table 2 shows the Performance evaluation of proposed method in presence of Gaussian noise [16]

Video	Spatial Domain	Frequency Domain	Proposed Method
PSNR (db)	49	44	59
NCC	0.56	0.75	0.94
BER	0.65	0.32	0.03

Method	Advantages	Disadvantages
Discrete Wavelet Transform (DWT) Schur Decomposition [1]	Excellent Spatial frequency analysis. Good energy compaction Robust signal attacks. Higher compression ratio.	Less robustness against geometric attacks. Noise near edges of images or video frames.
Dual-Tree Complex Wavelet Transform Binary signature.[2]	Proved efficiency to ensure robust watermarking. The robustness did not affect the visual quality of the tested videos.	Failed to extract binary signature extraction. Other attacks have led to a wrong interpretation of some bits
Discrete Cosine Transform (DCT) [5]	Increases the imperceptibility. Good performance in terms of robustness	Limited protection against geometric attacks. Block effect Computationally expensive.
Discrete Wavelet Transform (DWT) Alpha blending Technique. [3]	Robust Schema depends on high PSNR and low MSE.	Redundancy makes it more vulnerable to attacks.
Three-dimensional (3D) Cosine Transform. [7]	Higher robustness and obscurity	Block effect
Dual-Tree Complex Wavelet Transform ”DT-CWT”. [4]	Imperceptible and robust to Additive White Gaussian Noise (AWGN)	Limited protection against geometric attacks.
Discrete Wavelet Transform "DWT" Singular Value Decomposition “SVD” [8]	Robustness are high imperceptibility against different pictures and videos preparing assaults.	Computational cost
Arnold Transform "AT" Homomorphic Transform "HT". [10]	Resistance against geometric and signal processing attacks (high robustness) high imperceptibility.	Lacks shift-invariance, Computationally expensive.
Singular Value Decomposition (SVD) [6]	The compromise between robustness and quality is achieved. Robustness against various attacks quality.	Poor retrieval accuracy. Computationally expensive.
Discrete Wavelet Transform "DWT" [9]	Good resistance against geometric and signal processing attacks High energy compaction.	High false positive outcomes. Computationally expensive.

Table 3 Previous researches carried out in the watermarking domain with the adopted methods and their advantages & limitations.

VII. Conclusion

Different watermarking algorithms for video have been investigated, with a focus on spatial and frequency domain methods. The study's objective is to outline a straightforward framework for digital watermark technology. The question of copyright protection for digital work can really be raised in relation to a digital watermark. It's hard to keep your watermark secure. This analysis revealed that putting the watermark in the frequency domain offered more protection against potential violations.

The style of the watermark should feature straightforward forms and textures as a need for the invisible watermark embedding method to preserve raw image detail. The authorized owner won't be able to defend their presence from the unauthorized attacks if watermark forms are deformed without significantly changing the original stored image.

VIII. Acknowledgments

We would like to express our sincere gratitude to our college especially our E&TC department for providing an opportunity to work on the project. We would like to convey our heartfelt gratitude to Dr. M. A. Gangarde for his tremendous support and assistance in the completion of survey paper of our project and constantly encouraging and guiding us throughout the semester without which completing out required project work in short span could not be possible. His initial guidance regarding the study of several research papers related to our project helped us a lot while completing our project

IX. References

1. L. Rajab, T. Al-Khatib, and A. Al-Haj, "A blind DWT-SCHUR based digital video watermarking technique," J. Softw. Eng. Appl., vol. 8, no. 04, p. 224, 2015.

2. P. Senatore, A. Piva, F. Garzia, and R. Cusani, "A Blind Video Watermarking Algorithm for Copyright Protection based on Dual Tree Complex Wavelet Transform." Journal of Information Hiding and Multimedia Signal Processing, vol. 7, no. 6, 2016

3. S. A. Thajeel, "Robust Video Watermarking of Hybrid Based Techniques," Iraqi J. Sci., pp. 2458–2466, 2017

4. T. Aggarwal and N. Kaur, "Video Watermarking using Discrete Wavelet Transformation," International Research Journal of Engineering and Technology, vol. 7, 2020.

5. N. Asha and P. Bhagya, "An Efficient Fingerprint Watermarking Approach Using 3 Levels DWT and Alpha Blending Technique," Imp. J. Interdiscip. Res., vol. 2, 2016.

6. S. B. Latha, D. V. Reddy, and A. Damodaram, "Robust Video Watermarking using Secret Sharing and Cuckoo Search Algorithm," International Journal of Innovative Technology and Exploring Engineering, vol. 8, 2019

7. M. Ghalejughi and M. A. Akhaee, "Video watermarking in the DT-CWT domain using hyperbolic function," in 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), 2016, pp. 97–100

8. S. V Belim and P. G. Cherepanov, "Digital video watermarking algorithm robust against video j_container format changes," in Journal of Physics: Conference Series, 2019, vol. 1260, no. 2, p. 22001.

9. N. Revathi and M. Rukmani, "Hierarchical Clustering Based Medical Video Watermarking Using DWT and SVD," in International Conference on Emerging Current Trends in Computing and Expert Technology, 2019, pp. 792–805.

10. P. Khare and V. K. Srivastava, "A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT," J. Intell. Syst., vol. 30, no. 1, pp. 297–311, 2020.

11. M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 9, pp. 2131–2153, 2017.

12. L. H. Zhang, C. Yang, X. W. Kong, "Video Watermarking Synchronization Based on Motion Vector Statistics", Journal of Optoelectronics·Laser, Vol.18, No.2, Feb. 2007, pp, 236-240.

13. G. C.-W. Ting, B.-M. Goi, and S.-W. Lee, ''Robustness attacks on video watermarking using singular value decomposition,'' in Proc. 3rd Int. Conf. Digit. Signal Process., 2019, pp. 157–162.

14. X. Yu, C. Wang, and X. Zhou, "A survey on robust video watermarking algorithms for copyright protection," Applied Sciences, vol. 8, no. 10, p. 1891, 2018.

15. M. A. Gangarde and J. S. Chitode, "Application of Crypto-Video Watermarking Technique to Improve Robustness and Imperceptibility of Secret Data" pp.978-1-5090-6734, 2017.

16. Bushra Abdulla N. T and K. A. Navas, " Robust Video Watermarking Resilient To Inadvertent Attacks" pp. 978-1-7281-8396, 2020.